

March 27, 2024

VIA EMAIL

Anthony G. Brown
Office of the Attorney General
Attn: Security Breach Notification
200 St. Paul Place
Baltimore, Maryland 21202

Email: idtheft@oag.state.md.us

Re: Notice of Data Security Incident

Dear Attorney General Brown:

Constangy, Brooks, Smith & Prophete, LLP (“Constangy”) represents The Woodlands Methodist Church (“TWMC”) in connection with a recent data security incident described in greater detail below. The purpose of this letter is to notify you of the incident in accordance with Maryland’s data breach notification statute.

1. Nature of the Security Incident

On March 29, 2023, TWMC discovered it was the victim of a sophisticated cybersecurity attack affecting its network environment. Upon discovering this activity, TWMC took immediate steps to secure its computer network. TWMC also engaged a leading cybersecurity firm to assist with a forensic investigation to determine what happened and evaluate the extent of any unauthorized activity. After a thorough review of the potentially affected files, on or about February 2, 2024, TWMC confirmed that personal information for certain individuals may have been impacted. TWMC then immediately began collecting up-to-date contact information for potentially impacted individuals and arranged for notification letters to be sent as soon as possible.

2. Number of Affected Maryland Resident(s) & Information Involved

The incident involved personal information for approximately one (1) Maryland resident. The information involved in the incident for affected Maryland resident may have included name and Social Security number.

3. Notification to Affected Individuals

On March 27, 2024, a notification letter was sent to the affected Maryland resident by USPS First Class Mail. The notification letter provides resources and steps this individual can take to help protect their information. The letter also offers those individuals whose Social Security number was affected by the incident the opportunity to enroll in 12 months of complimentary identity protection services, including credit monitoring, \$1,000,000 insurance reimbursement policy, and fully managed identity theft recovery reservices. A sample notification letter sent to the impacted individuals is included with this correspondence.

4. Steps Taken Relating to the Incident

In response to the incident, TWMC retained cybersecurity experts and launched a forensics investigation to determine the source and scope of the compromise. TWMC also implemented additional security measures to further harden its digital environment in an effort to prevent a similar event from occurring in the future. Additionally, TWMC reported the incident to the FBI and will cooperate with any resulting investigation.

Finally, TWMC is notifying the affected individual and providing them with steps they can take to protect their personal information as discussed above.

5. Contact Information

If you have any questions or need additional information, please do not hesitate to contact me at lgodfrey@constangy.com or 973.462.9521, or David Rice at or drice@constangy.com or 718.614.2656.

Best regards,

Lauren D. Godfrey

Lauren Godfrey

CONSTANGY, BROOKS, SMITH & PROPHETE, LLP

Enclosure: Sample Notification Letter



Secure Processing Center
25 Route 111, P.O. Box 1048
Smithtown, NY 11787

<<First Name>> << Last Name>>
<<Address 1>>
<<Address 2>>
<<City>>, <<State>> <<Zip Code>>
<<Country>>

<<Date>>

Subject: Notice of Data <<Breach/Security Incident>>:

Dear <<First Name>> << Last Name>>:

I am writing to inform you of a data security incident experienced by The Woodlands Methodist Church ("TWMC") that may have affected your personal information. Please read this letter carefully as it contains important details about the incident and resources you may utilize to help protect your personal information. TWMC takes this matter extremely seriously as the security of our networks and the information we store is of paramount importance.

What Happened? On March 29, 2023, TWMC discovered it was the victim of a sophisticated cybersecurity attack affecting our network environment. Upon discovering this activity, we took immediate steps to secure our computer network. We also engaged a leading cybersecurity firm to assist with a forensic investigation to determine what happened and evaluate the extent of any unauthorized activity. After a thorough review of the potentially affected files, on or about February 2, 2024, we confirmed that personal information for certain individuals may have been impacted. We then immediately began collecting up-to-date contact information for potentially impacted individuals and arranged for notification letters to be sent as soon as possible.

What Information Was Involved? The potentially affected information may have included your name and <<Data Elements>>. Please note that TWMC has no evidence that any of this information has been misused.

What Are We Doing? As soon as we discovered this incident, we took steps to secure our environment and enlisted a leading cybersecurity firm to conduct a forensic investigation. We have also implemented additional security measures to help reduce the risk of a similar incident occurring in the future. In addition, we notified the Federal Bureau of Investigation and will cooperate with any resulting investigation.

In addition, out of an abundance of caution, we are offering you complimentary credit monitoring and identity theft protection services through Equifax – a data breach and recovery services expert. These services include: <<12/24>> months of Equifax Credit Watch Gold¹ with credit monitoring, a \$1,000,000 insurance reimbursement policy, WebScan notifications, and fully managed id theft recovery services. With this protection, Equifax will help you resolve issues if your identity is compromised. Please note that the deadline to enroll is <<Enrollment Deadline>>.

What Can You Do? TWMC recommends that you review the guidance included with this letter about how to protect your information. You can also enroll in the complimentary identity protection services being offered to you by using the Enrollment Code provided above.

¹ To receive credit monitoring services, you must be over the age of 18 and have established credit in the U.S., have a Social Security number in your name, and have a U.S. residential address associated with your credit file.

For More Information: Further information about how to help protect your information appears on the following page. If you have questions about this matter or need assistance enrolling in the complimentary services being offered to you, please call 1-844-694-4644 from 8:00 A.M. to 8:00 P.M. Central Time, Monday through Friday (excluding holidays).

We take your trust in us and this matter very seriously. Please accept our sincere apologies for any worry or inconvenience that this may cause you.

Sincerely,

A handwritten signature in black ink, appearing to read "Drew Essen". The signature is fluid and cursive, with the first name "Drew" being more prominent than the last name "Essen".

Rev. Drew Essen
Executive Pastor
The Woodlands Methodist Church
2200 Lake Woodlands Dr
The Woodlands, TX 77380 USA

Steps You Can Take to Protect Your Personal Information

Review Your Account Statements and Notify Law Enforcement of Suspicious Activity: As a precautionary measure, we recommend that you remain vigilant by reviewing your account statements and credit reports closely. If you detect any suspicious activity on an account, you should promptly notify the financial institution or company with which the account is maintained. You also should promptly report any fraudulent activity or any suspected incidence of identity theft to proper law enforcement authorities, your state attorney general, and/or the Federal Trade Commission (FTC).

Request a Copy of Your Credit Report: You may obtain a free copy of your credit report from each of the three major credit reporting agencies once every 12 months by visiting <https://www.annualcreditreport.com>, calling toll-free 1-877-322-8228, or by completing an Annual Credit Report Request Form and mailing it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348. You also can contact one of the following three national credit reporting agencies:

Equifax

P.O. Box 105851
Atlanta, GA 30348
1-800-525-6285
www.equifax.com

Experian

P.O. Box 9532
Allen, TX 75013
1-888-397-3742
www.experian.com

TransUnion

P.O. Box 1000
Chester, PA 19016
1-800-916-8800
www.transunion.com

Place a Fraud Alert: You may want to consider placing a fraud alert on your credit report. An initial fraud alert is free and will stay on your credit file for at least one year. The alert informs creditors of possible fraudulent activity within your report and requests that the creditor contact you prior to establishing any accounts in your name. To place a fraud alert on your credit report, contact any of the three credit reporting agencies identified above. Additional information is available at <https://www.annualcreditreport.com>.

Put a Security Freeze: You have the right to put a security freeze on your credit file for up to one year at no cost. This will prevent new credit from being opened in your name without the use of a PIN number that is issued to you when you initiate the freeze. A security freeze is designed to prevent potential creditors from accessing your credit report without your consent. As a result, using a security freeze may interfere with or delay your ability to obtain credit. You must separately place a security freeze on your credit file with each credit reporting agency. In order to place a security freeze, you may be required to provide the consumer reporting agency with information that identifies you, including your full name, Social Security Number, date of birth, current and previous addresses, a copy of your state-issued identification card, and a recent utility bill, bank statement or insurance statement.

Additional Free Resources: You can obtain information from the consumer reporting agencies, the FTC, or from your respective state Attorney General about fraud alerts, security freezes, and steps you can take toward preventing identity theft. You may report suspected identity theft to local law enforcement, including to the FTC or to the Attorney General in your state.

Federal Trade Commission (FTC)

600 Pennsylvania Ave, NW
Washington, DC 20580
consumer.ftc.gov, and
www.ftc.gov/idtheft
1-877-438-4338

Maryland Attorney General

200 St. Paul Place
Baltimore, MD 21202
oag.state.md.us
1-888-743-0023

New York Attorney General

Bureau of Internet and Technology
Resources
28 Liberty Street
New York, NY 10005
1-212-416-8433

North Carolina Attorney General

9001 Mail Service Center
Raleigh, NC 27699
ncdoj.gov
1-877-566-7226

Rhode Island Attorney General

150 South Main Street
Providence, RI 02903
<http://www.riag.ri.gov>
1-401-274-4400

Washington D.C. Attorney General

441 4th Street, NW
Washington, DC 20001
oag.dc.gov
1-202-727-3400

You also have certain rights under the Fair Credit Reporting Act (FCRA): These rights include to know what is in your file; to dispute incomplete or inaccurate information; to have consumer reporting agencies correct or delete inaccurate, incomplete, or unverifiable information; as well as other rights. For more information about the FCRA and your rights pursuant to the FCRA, please visit http://files.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf.



<<First Name>> <<Last Name>>

Enter your Activation Code: <<ACTIVATION CODE>>

Enrollment Deadline: <<Enrollment Deadline>>

Equifax Credit Watch™ Gold

*Note: You must be over age 18 with a credit file to take advantage of the product

Key Features

- Credit monitoring with email notifications of key changes to your Equifax credit report
- Daily access to your Equifax credit report
- WebScan notifications¹ when your personal information, such as Social Security Number, credit/debit card or bank account numbers are found on fraudulent Internet trading sites
- Automatic fraud alerts², which encourages potential lenders to take extra steps to verify your identity before extending credit, plus blocked inquiry alerts and Equifax credit report lock³
- Identity Restoration to help restore your identity should you become a victim of identity theft, and a dedicated Identity Restoration Specialist to work on your behalf
- Up to \$1,000,000 of identity theft insurance coverage for certain out of pocket expenses resulting from identity theft⁴

Enrollment Instructions

Go to www.equifax.com/activate

Enter your unique Activation Code of <<ACTIVATION CODE>> then click “Submit” and follow these 4 steps:

1. **Register:**

Complete the form with your contact information and click “Continue”.

If you already have a myEquifax account, click the ‘Sign in here’ link under the “Let’s get started” header.

Once you have successfully signed in, you will skip to the Checkout Page in Step 4

2. **Create Account:**

Enter your email address, create a password, and accept the terms of use.

3. **Verify Identity:**

To enroll in your product, we will ask you to complete our identity verification process.

4. **Checkout:**

Upon successful verification of your identity, you will see the Checkout Page.

Click ‘Sign Me Up’ to finish enrolling.

You’re done!

The confirmation page shows your completed enrollment.

Click “View My Product” to access the product features.

¹WebScan searches for your Social Security Number, up to 5 passport numbers, up to 6 bank account numbers, up to 6 credit/debit card numbers, up to 6 email addresses, and up to 10 medical ID numbers. WebScan searches thousands of Internet sites where consumers' personal information is suspected of being bought and sold, and regularly adds new sites to the list of those it searches. However, the Internet addresses of these suspected Internet trading sites are not published and frequently change, so there is no guarantee that we are able to locate and search every possible Internet site where consumers' personal information is at risk of being traded. ²The Automatic Fraud Alert feature is made available to consumers by Equifax Information Services

LLC and fulfilled on its behalf by Equifax Consumer Services LLC. ³Locking your Equifax credit report will prevent access to it by certain third parties. Locking your Equifax credit report will not prevent access to your credit report at any other credit reporting agency. Entities that may still have access to your Equifax credit report include: companies like Equifax Global Consumer Solutions, which provide you with access to your credit report or credit score, or monitor your credit report as part of a subscription or similar service; companies that provide you with a copy of your credit report or credit score, upon your request; federal, state and local government agencies and courts in certain circumstances; companies using the information in connection with the underwriting of insurance, or for employment, tenant or background screening purposes; companies that have a current account or relationship with you, and collection agencies acting on behalf of those whom you owe; companies that authenticate a consumer's identity for purposes other than granting credit, or for investigating or preventing actual or potential fraud; and companies that wish to make pre-approved offers of credit or insurance to you. To opt out of such pre-approved offers, visit www.optoutprescreen.com ⁴The Identity Theft Insurance benefit is underwritten and administered by American Bankers Insurance Company of Florida, an Assurant company, under group or blanket policies issued to Equifax, Inc., or its respective affiliates for the benefit of its Members. Please refer to the actual policies for terms, conditions, and exclusions of coverage. Coverage may not be available in all jurisdictions.